Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0486

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Fortinet FortiClient en FortiClien-tEMS

Publicatiedatum: 12-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Fortinet heeft kwetsbaarheden verholpen in FortiClient en FortiClientEMS.

Duiding

In FortiClientEMS kunnen geauthenticeerde lokale gebruikers met administratieve rechten hun toegang escaleren naar een root shell door het uitvoeren van CLI-commando's met te hoge privileges. Dit komt doordat de commando's meer rechten krijgen dan noodzakelijk, wat root-level controle mogelijk maakt. Deze kwetsbaarheid betreft het FortiClientEMS managementsysteem en kan de integriteit van beheerde endpoints beïnvloeden. Daarnaast bestaat er in FortiClient voor Mac en Windows een kwetsbaarheid in de origin validation mechanism. Een niet-geautoriseerde externe aanvaller kan hierdoor willekeurige code of commando's uitvoeren op het getroffen systeem, mits het slachtoffer interactie toont, zoals het klikken op een kwaadaardige link of het openen van een speciaal vervaardigd bestand. De oorzaak ligt in een onjuiste validatie van de oorsprong, waardoor beveiligingscontroles kunnen worden omzeild.

Oplossingen

Fortinet heeft updates uitgebracht om de kwetsbaarheden in FortiClient en FortiClientEMS te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.fortiguard.com/psirt/FG-IR-26-192
- https://www.fortiguard.com/psirt/FG-IR-26-194

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-121527	6.7 MEDIUM
CVE-2026-121529	9.6 CRITICAL

CWE's

CWE	Beschrijving
CWE-250	Execution with Unnecessary Privileges
CWE-346	Origin Validation Error

Getroffen producten

Fortinet
FortiClient
FortiClientEMS

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.